

Manajemen Risiko Sistem Informasi Rumah Sakit Menggunakan Framework NIST SP 800-30 (Studi Kasus: RSIA Eria Bunda Pekanbaru)

Fuadi Khalish Muttaqi

Ilmu Komputer, Universitas Muhammadiyah Riau
email: fuadi.khalish@gmail.com

Abstract

In the midst of advances in information technology as it is today, IT systems and assets in hospitals are crucial in providing the information needed. In the application of hospital information systems there are certainly risks that threaten the sustainability of the information system, one of the causes is the organization's failure to assess the source of the risk threat. The risk can be in the form of events or events that result in disruption even the cessation of information system services to the hospital. The purpose of this study is to determine the risks that could occur in the hospital information system RSIA Eria Bunda (GRAPHASoft) using the NIST SP 800-30 framework by means of risk assessment, risk mitigation and risk evaluation, as well as providing recommendations to minimize risk risks identified in the Eria Bunda RSIA information system. Based on research risk that must be prioritized is the server overhead computer, because this risk has the most quantity based on existing vulnerabilities, the remaining risks such as hardware damage, server down, loss of data, information accessed by others, misuse of user ID, former employee still have access rights, unauthorized physical access, data leakage and virus attacks have a value of one quantity each. Risk mitigation that must be done by RSIA Eria Bunda is by procuring a server-specific computer and providing a server-specific room to avoid the highest risk identified.

Keywords: Risk management, NIST SP 800-30, Hospital, Information System.

Abstrak

Di tengah kemajuan teknologi informasi seperti saat ini, sistem dan aset TI pada rumah sakit menjadi hal yang krusial pada penyediaan informasi yang di butuhkan. Pada penerapan sistem informasi rumah sakit pastinya ada risiko yang mengancam keberlangsungan sistem informasi tersebut, salah satu penyebab nya adalah kegagalan organisasi dalam menilai sumber ancaman risiko. Risiko bisa saja berupa peristiwa atau kejadian yang mengakibatkan terganggu bahkan terhentinya layanan sistem informasi kepada rumah sakit tersebut. Tujuan dari penelitian ini adalah untuk mengetahui risiko-risiko yang bisa saja terjadi pada sistem informasi rumah sakit RSIA Eria Bunda (GRAPHASoft) dengan menggunakan framework NIST SP 800-30 dengan cara penilaian risiko, mitigasi risiko dan evaluasi risiko, sekaligus memberikan rekomendasi untuk meminimalisir risiko-risiko yang teridentifikasi pada sistem informasi RSIA Eria Bunda. Berdasarkan penelitian risiko yang harus di prioritaskan adalah komputer server overhead, karna risiko ini memiliki kuantitas paling banyak berdasarkan kerentanan yang ada, sisanya risiko seperti kerusakan hardware, server down, hilangnya data, informasi diakses oleh orang lain, penyalahgunaan user id, mantan pekerja masih memiliki hak akses, akses fisik yang tidak terotorisasi, kebocoran data dan serangan virus memiliki nilai masing-masing satu kuantitas. mitigasi risiko yang harus di lakukan RSIA Eria Bunda adalah dengan melakukan pengadaan komputer khusus server dan pengadaan ruangan khusus server untuk menghindari risiko tertinggi yang teridentifikasi.

Keywords: Manajemen Risiko, NIST SP 800-30, Rumah Sakit, Sistem Informasi.

PENDAHULUAN

Di tengah kemajuan teknologi seperti saat ini, kebutuhan informasi yang tepat dan akurat sangatlah diperlukan, bagi instansi pemerintahan, perkantoran, dunia kerja maupun dunia kesehatan. Aktivitas mengelola data menjadi sebuah informasi yang tepat dan memiliki daya guna adalah hal yang krusial pada penyediaan informasi yang dibutuhkan. begitu juga dalam hal pelayanan kesehatan seperti pelayanan rumah Sakit. Rumah sakit harus membuat pelaporannya agar aktivitas pelayanan rumah sakit tertata dengan baik. Pelaporan rumah sakit yang baik sangat berhubungan dengan pengelolaan data rumah sakit sehingga rumah sakit membutuhkan sebuah sistem informasi yang manajemen dan mengawasi pengisian dan pengelolaan data rumah sakit itu sendiri maka diperlukan sebuah Sistem Informasi Rumah Sakit (SIRS).

Hambatan-hambatan yang terjadi dan mengganggu sistem informasi pada umumnya di nyatakan sebagai risiko. Risiko bisa saja terjadi dari macam-macam kejadian dan kondisi yang terjadi pada lingkup sistem informasi rumah sakit yang berdampak buruk bagi rumah sakit itu sendiri. Rumah Sakit Ibu dan Anak Eria Bunda sebelumnya tidak pernah melaksanakan kegiatan penilaian risiko pada lingkup sistem informasi yang mereka gunakan, pada Rumah Sakit Ibu dan Anak Eria Bunda sistem informasi hanya di gunakan sebagai sarana layanan informasi tanpa melakukan pencegahan ancaman risiko yang bisa saja mengancam keberlangsungan sistem informasi rumah sakit, sedangkan sistem informasi rumah sakit pada Rumah Sakit Ibu dan Anak Eria Bunda telah menjadi bagian yang penting dan sama sekali tidak bisa di pisahkan pada kegiatan dan proses layanan maupun pengelolaan data yang dilakukan rumah sakit. Seandainya terjadi gangguan pada sistem informasi rumah sakit milik Rumah Sakit Ibu dan Anak Eria Bunda, maka layanan informasi menjadi terganggu yang bisa berakibat keberlangsungan pelayanan rumah sakit juga terganggu.

Berdasarkan penjelasan diatas, maka penelitian ini bertujuan untuk mengukur risiko sistem informasi Rumah Sakit Ibu dan Anak Eria Bunda dengan judul “Manajemen Risiko Sistem Informasi Rumah Sakit Menggunakan *Frame Work* NIST SP 800-30 (Studi Kasus:

RSIA Eria Bunda)”. Dari hasil penelitian diharapkan dapat memberikan informasi kepada pihak berwenang tentang memahami, menilai dan mengambil tindakan pada semua risiko sistem informasi dengan maksud untuk meningkatkan kemungkinan keberhasilan dan mengurangi kemungkinan kegagalan tujuan organisasi.

TINJAUAN PUSTAKA

Risiko

Pada sebuah organisasi atau pemerintahan risiko bisa di artikan sebagai apapun tindakan yang bisa berpengaruh pada tercapainya visi organisasi. Menurut para ahli Risiko pada buku *Fundamentals of Risks Management: Understanding, Evaluating and Implementing Effective Risk Management* milik Paul Hopkin risiko di definisikan sebagai (Hopkin, 2010:12): Pengaruh ketidakpastian terhadap suatu tujuan. Dimana efek tersebut mungkin positif, negatif, atau penyimpangan dari yang diharapkan.

Menurut (Pinontoan, 2010) risiko adalah dampak buruk dari sebuah peristiwa atau suatu pilihan yang dilakukan dalam kehidupan sehari-hari. (Darmawi, 2006) mengartikan risiko sebagai potensi untuk terjadinya hal negatif atau akibat yang merugikan, seperti potensi untuk kehilangan, cedera, kebakaran dan lain-lain.

Menurut pendapat (Gondodiyoto, 2007), risiko adalah sebuah kesempatan timbulnya akibat buruk pada pelaksanaan suatu celah, mempertimbangkan peluang dan akibat dari risiko. organisasi dapat meminimalisir risiko dengan menerapkan antisipasi berupa kontrol, tapi tidak akan bisa sepenuhnya menghilangkan adanya *exposure*, bahkan dengan struktur pengendalian penuh sekalipun. Sedangkan pendapat (Idroes, 2008), mengartikan risiko adalah bahaya, risiko adalah ancaman atau kemungkinan suatu pelakuan yang mendatangkan dampak yang berlawanan dengan visi organisasi.

Jadi dapat di simpulkan risiko adalah suatu potensi kejadian yang bisa merugikan organisasi atau perorangagn sehingga menyebabkan tidak tercapainya tujuan dan visi yang diinginkan karna adanya ketidakpastian. Pada risiko tidak ada metode apapun yang bisa menjamin 100% bahwa dampak negatif itu dapat di hindari setiap saat, terkecuali jika

aktifitas yang terdapat unsur risiko tidak dilaksanakan.

Manajemen Risiko

Menurut pendapat (Joint Task Force Transformation Initiative, 2011) manajemen risiko adalah proses dengan tujuan untuk memperoleh keseimbangan antara ketepatan dan mewujudkan peluang untuk memperoleh keuntungan dan memperkecil celah dan kerugian. Manajemen risiko harus dilaksanakan terus-menerus dan berulang yang terdiri dari beberapa langkah, ketika dilaksanakan dengan benar berkemungkinan terjadinya perbaikan secara terus menerus dalam pengambilan keputusan dan peningkatan kinerja.

Menurut pendapat (Stoneburner, 2002) Manajemen risiko adalah aktifitas yang memungkinkan manajer senior TI untuk menstarakan biaya operasional dan biaya ekonomi untuk aktifitas pengamanan pada usaha melindungi teknologi informasi dan data yang berperan pada misi organisasi.

Menurut pendapat (Blokdiik, 2008) manajemen risiko adalah sebuah langkah dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya adalah aktifitas untuk mengurangi dampak dari kerugian karna bencana pada biaya yang paling bisa diterima. agar memenuhi kebutuhan spesifik organisasi, kesuksesan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan memperhatikan visi, misi, dan tujuan organisasi.

Menurut pendapat (Gibson, 2011) manajemen risiko adalah praktik mengidentifikasi, menilai, mengendalikan, dan memitigasi risiko

Menurut pendapat (Maulana, 2006) manajemen risiko TI diharapkan bisa meminimalisir dampak kerusakan seperti, dampak terhadap keuangan, jelek nya reputasi yang dikarnakan oleh sistem yang tidak aman, berhentinya aktifitas bisnis, kegagalan inventaris yang dapat diidentifikasi (sistem dan data) dan pengunduran aktifitas pengambilan keputusan.

Menurut pendapat (Djojosoedarso, 2009) manajemen risiko adalah pelaksanaan tujuan manajemen pada penanggulangan risiko, yaitu risiko yang terjadi pada perusahaan/

organisasi, masyarakat dan keluarga. Manajemen risiko mencakup kegiatan perencanaan, mengorganisir, menyusun, memimpin/ mengkoordinir dan monitoring (termasuk mengevaluasi) aktifitas penanggulangan risiko.

Menurut pendapat (Hanafi, 2009) pada dasarnya manajemen risiko dilaksanakan dengan proses identifikasi risiko, evaluasi, pengukuran risiko dan pengelolaan.

Menurut pendapat (Jordan, 2005) manajemen risiko adalah identifikasi dari ancaman dan penerapan dari perhitungan yang ditujukan pada pengurangan peristiwa ancaman tersebut dan mengurangi tiap kerusakan.

Menurut pendapat (Nugraha, 2016) manajemen risiko adalah suatu aktifitas yang memungkinkan pimpinan kelompok atau organisasi agar dapat menyeimbangkan biaya operasional dan ekonomi yang di alokasikan untuk meminimalisir risiko dan memperoleh keuntungan dengan melindungi sistem teknologi informasi dan data yang di butuhkan untuk menjalan visi, misi dan tujuan bisnis.

Sistem Informasi

Menurut pendapat (Oetomo, 2002) sistem Informasi adalah sekumpulan elemen yang saling terhung satu dengan yang lain menjadi sebuah satu kesatuan dengan tujuan mengintegrasikan data, memproses dan menyimpan serta mendistribusikan informasi. Sedangkan menurut pendapat (Indrajit, 2000) sistem informasi adalah sekumpulan dari komponen di organisasi atau perusahaan yang saling berhubungan. dengan proses penciptaan dan pengaliran informasi.

Menurut pendapat (Tantra, 2012) sistem informasi adalah suatu cara yang terorganisir, untuk mengumpulkan, memasukkan, dan memproses data dan menyimpannya mengelola, mengontrol dan melaporkannya sehingga dapat mendukung perusahaan atau organisasi untuk mencapai tujuan.

Menurut (Jogiyanto, 2005) sistem Informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi, dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Penelitian dilakukan dengan teliti, mendalam dan menyeluruh dengan cara melakukan wawancara mendalam dan pengamatan langsung (observasi) serta mendeskripsikan hal-hal yang berkaitan dengan obyek penelitian. hal utama yang diteliti yaitu manajemen risiko sistem informasi RSIA Eria Bunda dengan menggunakan kerangka kerja NIST SP 800-30. bila dilihat dari tujuan penelitian, jenis penelitian ini adalah studi kasus.

Tahapan Merencanakan

Pada tahap ini, mengidentifikasi masalah dan menentukan apa saja data yang dibutuhkan untuk melakukan penelitian. Berikut ini adalah penjabaran dari tiap tahap perencanaan:

1. Identifikasi Masalah,

Teknik pengumpulan data pada penelitian ini menggunakan wawancara dan observasi langsung pada tempat studi kasus, sekaligus mendeskripsikan hal-hal yang berhubungan dengan objek penelitian. Hal yang paling utama untuk di kaji adalah melakukan penilaian atas risiko yang terjadi dan bisa saja terjadi pada sistem informasi RSIA Eria Bunda menggunakan *frame work* NIST SP 800-30. Pengamatan ini di tujujukan terhadap kepala TI dan anggota selaku penanggung jawab lingkup TI di RSIA Eria Bunda yang nantinya merekalah yang akan melakukan manajemen risiko terhadap lingkup sistem informasi di RSIA Eria Bunda.

2. Pemilihan Kasus

Alasan pemilihan tempat peneitian di RSIA Eria Bunda adalah rumah sakit ini sudah menerapkan sistem informasi untuk melayani informasi dan sistem ini sudah berfungsi seutuhnya sehingga rumah sakit sangat bergantung pada keberlangsungan sistem informasi ini. Dan alas an yang kedua adalah RSIA Eria Bunda belum pernah menerapkan manajemen risiko pada lingkup TI nya agar dapat meminimalisir risiko atau ketidak pastian yang akan terjadi.

3. Menentukan Kebutuhan Data

Dimana pada tahap ini akan ditentukan data-data apa saja yang dibutuhkan pada penelitian ini. Dimana penentuan data yang ingin diambil setelah melakukan studi pendahuluan yaitu observasi pada RSIA Eria Bunda. Guna untuk membantu menentukan data seperti apa yang diperlukan dalam manajemen risiko sitem informasi rumah sakit.

Tahap Pengumpulan Data

Tahap pengumpulan data dilakukan dengan cara melakukan penggalian informasi dari pihak-pihak yang terlibat dalam sistem informasi tersebut penggalian informasi dilakukan dengan observasi dan wawancara. Berikut adalah Teknik pengumpulan data yang ada pada penelitian ini:

1. Observasi

Obsevasi adalah akitifitas mengamati langsung kondisi objek yang akan di teliti. Pada tahap ini, dilakukan *survey* secara langsung dengan mengunjungi RSIA Eria Bunda untuk melihat dan mengamati teknologi sistem informasi yang digunakan, resiko yang pernah dialami dan bagaimana proses yang dijalankan pihak menejemen resiko Rumah sakit dalam mendukung proses bisnis yang berjalan.

2. Wawancara

Tahap wawancara dilakukan di bagian IT RSIA Eria Bunda, yang tujuannya untuk mengidentifikasi masalah dan resiko yang pernah dialami. Wawancara di lakukan terhadap responden yang terbatas dengan cara menggali informasi yang kita butuhkan dari responden itu sendiri. Pengumpulan data lapangan terlebih dahulu dengan melaksanakan observasi tentang topik yang akan di teliti untuk lebih mendalami kajian.

Pada penelitian ini observasi dan wawancara dilaksanakan secara bersamaan, pengumpulan data di lakukan sebanyak dua kali, pengumpulan data pertama adalah untuk menentukan karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, dan analisis kontrol yang sudah di terapkan pada lingkup TI RSIA Eria Bunda, data hasil dari

pengumpulan data tahap pertama di proses berdasarkan framework NIST SP 800-30, output dari pengelolaan data ini berupa table karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, dan analisis kontrol. Setelah itu dilaksanakan kembali pengumpulan data menggunakan wawancara berdasarkan hasil pengelolaan data pertama, yang nantinya setelah dilakukan pengelolaan data ini akan menghasilkan table-tabel penilaian risiko sistem informasi RSIA Eria Bunda.

HASIL DAN PEMBAHASAN

Penilaian Risiko

1. Karakteristik Sistem

Inventaris TI disini dibagi menjadi lima bagian yaitu perangkat keras, perangkat lunak, informasi, infrastruktur dan sumber daya manusia.

Komponen-komponen yang ada pada karakteristik sistem adalah komputer server, komputer *client*, GRAPHASoft, Windows 10, Windows xp, Anti Virus (Kaspersky), Deep Freeze, database, CCTV, UPS, Pendingin udara, Instalasi Listrik, Genset, admin dan user GRA PPHASoft

2. Identifikasi Ancaman

Setelah melakukan observasi dan wawancara kepada kepala TI RSIA Eria Bunda, ditemukanlah beberapa ancaman yang pernah terjadi pada bagian TI RSIA Eria Bunda yaitu serangan virus, kegagalan backup data pada server, petugas salah melakukan input data, sambaran petir, pemadaman listrik tiba-tiba dan gangguan jaringan.

3. Identifikasi Kerentanan

Kerentanan yang terjadi di RSIA Eria Bunda antara lain Pemilihan perangkat komputer server yang kurang tepat, USB *port* yang tidak ter-*disable* pada komputer *client*, tidak ada kebijakan mengganti *password* user secara berkala, akun user yang sudah tidak aktif tidak di hapus sama sekali, tidak ada ketentuan jangka waktu *service* pendingin udara pada komputer server, belum memiliki ruang khusus untuk komputer server dan Backup rekaman CCTV hanya dalam jangka pendek.

4. Analisa Pengendalian

Kontrol yang sudah diterapkan pada TI RSIA Eria Bunda adalah Meng-*install* Anti virus pada komputer server, Meng-*install* Deep freeze pada komputer *client*, Penggunaan CCTV, Tersedia racun api, Tersedia genset, Memasang Anti Petir, Tiap user memiliki akun dan password sendiri dan adanya larangan merokok.

5. Penentuan Kemungkinan

Dari hasil wawancara, semua profil ancaman memiliki frekuensi yang rendah, salah satu ancaman besar yang pernah terjadi di lingkup TI RSIA Eria Bunda adalah sambaran petir, saat itu beberapa komputer client dan komputer server rusak, sehingga membuat aktifitas sistem informasi pada RSIA Eria Bunda menjadi berhenti bekerja. Selain dari ancaman itu ancaman yang pernah terjadi hanya ancaman kecil yang tidak mengganggu keberlangsungan sistem informasi RSIA Eria Bunda.

6. Analisa Dampak

Dari hasil wawancara terdapat beberapa ancaman dengan level tinggi yang bisa menghentikan keberlangsungan sistem informasi bahkan keberlangsungan aktifitas rumah sakit, seperti risiko akibat kejahatan manusia seperti *cybercrime*, pembajakan atau terorisme. Dan juga beberapa masalah pada komputer yang mengancam keberlangsungan sistem informasi seperti *server down* dan *overheat*. Dan yang terakhir risiko akibat bencana alam seperti kebakaran dan sambaran petir.

7. Penentuan Risiko

Penentuan risiko bertujuan untuk memberikan nilai tingkat dari risiko yang timbul pada lingkup TI, *input* dari langkah ini adalah tingkat dari *vulnerability* dan tingkat dari *impact* yang di petakan menjadi matrik 3x3 yang memiliki 3 level risiko yaitu rendah (low), sedang (medium) dan tinggi (high). Skor dari tiap level adalah:

Tabel 1. Level Probabilitas

Level	Nilai Probabilitas
1.0	Tinggi
0,5	Sedang
0,1	Rendah

Probabilitas untuk kecenderungan memiliki level 1.0 untuk tinggi, 0.5 untuk sedang dan 0.1 untuk rendah.

Tabel 2. Penilaian Dampak Risiko

Level	Nilai Risiko
100	Tinggi
50	Sedang
10	Rendah

Nilai untuk tiap dampak adalah 100 untuk tinggi, 50 untuk sedang dan 10 untuk rendah.

Tabel 3. Penentuan Risiko

Skor Risiko	Level Ranking
>50-100	Tinggi
>10-50	Sedang
1-10	Rendah

Nilai untuk tiap skor risiko adalah >50-100 untuk tinggi, >10-50 untuk sedang dan 1-10 untuk rendah.

Penilaian tingkat risiko pada sistem IT dilakukan pada langkah ini. Penentuan risiko ini bertujuan untuk menilai tingkat risiko terhadap sistem, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan. Risiko yang menentukan dapat dilihat pada tabel berikut ini:

$$\text{Penilaian Risiko} = \text{Dampak} \times \text{Kemungkinan}$$

8. Rekomendasi Pengendalian

Aktifitas ini emeberikan rekomendasi kontrol terhadap risiko yang telah di tentukan level nya. *Input* dari langah ini adalah risiko yang sudah di tentukan levelnya, dan di hasilkan lah daftar rekomendasi dari tiap risiko. Ada beberapa control yang sudah di diterapkan di bagian TI RSIA Eria Bunda seperti penggunaan ups dan stabilizer pada bebrapa perangkat TI, penggunaan ginset saat terjadinya pemadaman listrik, memasang CCTV pada beberapa titik di rumah sakit dan beberapa control lainnya. Selain itu rekomedasi kontrol di peroleh dari literatur yang harus di diterapkan di RSIA Eria Bunda agar dapat memperkecil level risiko.

9. Dokumentasi Hasil

Pada tahap ini, dilakukan pengumpulan laporan hasil penilaian risiko (karakteristik sistem, identifikasi ancaman, kerentanan, analisis control, penentuan kemungkinan, analisis dampak, penentuan risiko dan kontrol risiko). Merupakan laporan atau dokumentasi dari seluruh kegiatan yang ada, dimulai tahap karakteristik hingga rekomendasi kontrol.

Hasil dari penilaian risiko didokumentasikan berupa profil risiko yang dapat mengancam keberlangsungan sistem informasi, dan solusi pencegahan melalui rekomendasi kontrol sebagai tindak lanjut proses berikutnya melalui kegiatan mitigasi risiko.

Peringatan Risiko

1. Prioritas Aksi

Pada penelitian ini, untuk memperoleh prioritas aksi, dibandingkan seluruh daftar risiko yang sudah terdokumentasi dengan table analisis kerentanan. Risiko yang paling tinggi kuantitasnya pada kerentanan yang ada, itulah risiko yang akan di prioritaskan. Di bawah ini adalah table dari prioritas aksi:

Tabel 4. Prioritas Aksi

No	Risiko	Kuantitas
1.	<i>Overheat</i>	3
2.	Kegagalan atau kerusakan <i>hardware</i>	1
3.	<i>Server down</i>	1
4.	Hilangnya data	1
5.	Informasi Diakses oleh orang tidak berwenang	1
6.	Penyalahgunaan hak akses atau <i>user id</i>	1
7.	Mantan user atau karyawan masih memiliki akses informasi	1
8.	Akses fisik yang tidak terotorisasi	1
9.	Kebocoran data atau informasi internal	1
10.	Serangan virus	1

2. Opsi Evaluasi Rekomendasi Kontrol

Dari hasil rekomendasi kontrol yang ada pada tahap penilaian risiko, berikut adalah hasil dari evaluasi rekomendasi kontrol, karna rekomendasi kontrol sebelumnya belum tentu tepat dan sesuai dengan yang di butuhkan berdasarkan kerentanan.

Tabel 5. Evaluasi Kontrol

No	Tipe Risiko	Control Recommendation
1.	<i>Overheat</i>	Memperhatikan suhu dari perangkat TI terutama komputer server yang bekerja sangat keras 24 jam nonstop. Salah satu cara nya dengan membuat ruang khusus server sehingga dapat selalu menjaga suhu yang di butuhkan server.
2.	Kegagalan atau kerusakan <i>hardware</i>	Menghimbau untuk semua pengguna agar menjaga, merawat dan menggunakan dengan baik semua perangkat keras yang ada di rumah sakit dan juga memperhatikan pemilihan komponen pada komputer atau hardware sesuai dengan kebutuhan.
3.	<i>Server down</i>	a. Rutin membersihkan komponen dan perangkat keras dari komputer server b. Memperhatikan suhu komputer server untuk menghindari overhead c. Memperhatikan perangkat

		pendukung seperti kael LAN dan swtich Hub agar jaringan selalu berjalan dengan lancar.
4.	Hilangnya data	a. Memantau log aktivitas peng-inputan data secara berkala. b. Komputer server harus memiliki ruang kunic pengaman atau finger print untuk menghindari hilangnya data.
5.	Informasi Diakses oleh orang tidak berwenang	Menerapkan <i>Confidentiality</i> yaitu aktifitas menjamin bahwa data atau informasi hanya di akses oleh orang yang berwenang saja.
6.	Penyalah gunaan hak akses atau <i>user id</i>	a. Perubahan password secara berkala b. Kerahasiaan password c. Menghapus akun yang sudah tidak digunakan
7.	Mantan user atau karyawan masih memiliki akses informasi	Menghapus akun dan izin akses karyawan yang sudah tidak bekerja di rumah sakit secara langsung.
8.	Akses fisik yang tidak terotoritasi	Memberikan larangan yang tegas untuk tidak mengakses

		ruangan ataupun perangkat bagi orang yang tidak memiliki izin.
9.	Kebocoran data atau informasi internal	Menerapkan <i>Confidentiality</i> yaitu aktifitas menjamin bahwa data atau informasi hanya di akses oleh orang yang berwenang saja.
10.	Serangan virus	Menjadikan usb port disable sehingga tidak bisa menggunakan usb

3. Analisis Maanfaat biaya

Langkah ini bertujuan membantu manajer senior untk menentukan pilihan kontrol biaya yang paling efektif dan menganalisis keuntungan pada biaya nya. Yang di lakukan pada aktifitas ini adalah cost benefit analysis jika kontrol di terapkan pada sistem, dan jika kontrol tidak di terapkan pada sistem.

Belum ada anggaran atau dana khusus dialokasikan untuk pelaksanaan manajemen risiko pada TI RISA Eria Bunda, tetapi untuk risiko ataupun kejadian yang bersifat insidental, RSIA Eria Bunda masih dapat mengalokasikan dana untuk itu karena berhubungan dengan layanan yang tidak boleh terhenti.

4. Pemilihan Kontrol

Memilih kontrol yang paling baik secara teknis dan biaya pada hasil langkah sebelumnya yaitu *conduct cost benefit analysis*. Hasil dari langkah ini adalah kontrol yang dipilih dan akan di terapkan.

Pemilihan kontrol yang sebaiknya dilaksanakan oleh TI Rsia Eria Bunda adalah membuat ruang khusus untuk server yang memenuhi standardnya seperti memiliki pendingin udara yang cukup

yang bisa menjaga ruangan pada suhu 2 derajat selsius untuk menghindari *server overhead*. Selalu tertutup rapat dan terkunci bila perlu menggunakan kunci fingerprint dan CCTV untuk mengetahui siapa saja yang mengakses ruang server itu.

5. Tugas dan tanggung Jawab
Manajer senior menunjuk personil yang di kira cocok untuk melakukan dan mepertanggung jawabkan kontrol yang di terapkan pada sistem. Outputnya adalah penanggungjawab yang terpilih untuk melaksanakan kontrol terhadap sistem. Mitigasi risiko adalah proses yang berkelanjutan dan di lakukan secara terus menerus, di sini di butuhkan personil yang bertanggung jawab dan berkompeten di bidangnya. RSIA Eria Bunda sudah mempunyai devisi TI yang memiliki pemahaman dan kompeten dalam bidang teknologi inforamsi sebagai penanggung jawab untuk itu.
6. Pengembangan Rencana dan Perlindungan
Ini adalah aktifitas perencanaan terhadap implementasi kontrol yang di tentukan tadi agar dapat mempermudah proses mitigasi risiko. Pengembangan rencana perlindungan yang di rencanakan sesuai pada rekomendasi kontrol pada tahap penilaian risiko.
7. Implementasi Kontrol
Aktifitasi ini adalah menerapkan kontrol yang terpilih. *Input* nya adalah hasil dari tahap implementasi, sementara *outputnya* adalah pengurangan risiko.
Pada tahap ini RSIA Eria Bunda menerapkan kontrol sesuai opsi evaluasi kontrol. Hasil tersebut dapat dijadikan sebagai informasi bagi RSIA Eria Bunda untuk menyempurnakan penerapan teknologi informasi yang ada dan untuk dapat mendukung tujuan bisnisnya berupaya menghilangkan sumber risiko tersebut dengan berbagai kegiatan dan memperhatikan rekomendasi kontrol yang telah dilaksanakan.

Evaluasi Risiko

Evaluasi rirsiko adalah langkah yang di lakukan setelah berlangsungnya aktivitas peringanan. Karna seiring berjalan nya waktu aset-aset TI yang ad apada organisasi atau istitusi pasti akan berkembang atau mengalam

perubahan seperti pergantian komponen hardware ataupun software yang sudah di update ke yang terbaru.

Seharusnya RSIA Eria Bunda melakukan evaluasi risiko terus menerus selama rumah sakit ini berdiri, karna seiring berjalannya waktu aset-aset TI yang ada pada daftar karakteristik sistem akan berkembang seperti di update, upgread maupun ada perangkat yang di ganti, proses ini memastikan apakah aset TI yang sudah berkembang tadi masih bisa di implementasikan rekomendasi kontrol yang telah dibuat melalui model manajemen risiko ini. Seandainya ada aset TI yang sudah tidak bisa dilakukan rekomendasi kontrol terhadapnya, aset TI tersebut harus di data dan dilakukan proses penilaian risiko dan mitigasi risiko ulang sehingga manajemen risiko ini bersifat repetisi agar dapat selalu meminimalisir terjadinya ancaman risiko.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan penelelitian yang di lakukan pada RSIA Eria Bunda yaitu penelitian di lakukan dengan cara melakukan penilaian risiko terhadap keberlangsungan sistem informasi RSIA Eria Bunda dengan menggunakan framework NIST SP 800-30 dapat di simpulkan :

1. Pada langkah penilaian risiko (*risk assesement*) penelitian ini mendeskripsikan berbagai macam profil risiko dan melakukan penentuan risiko, sehingga TI RSIA Eria Bunda tau risiko mana yang harus di prioritaskan untuk di lakukan mitigasi risiko. Berdasarkan penelitian risiko yang harus di prioritaskan adalah komputer *server overhead*, karna risiko ini memiliki kuantitas paling banyak berdasarkan kerentanan yang ada, sisanya risiko seperti kerusakan hardware, *server down*, hilangnya data, inforamasi diakses oleh orang lain, penyalahgunaan *user id*, mantan pekerja masih memiliki hak akses, akses fisik yang tidak terotoritasi, kebocoran data dan serangan virus memiliki nilai masing-masing satu kuantitas. TI RSIA Eria Bunda sudah menerapkan beberapa kontrol seperti meng-*install* anti virus dan deepfreeze pada beberapa computer, penggunaan CCTV, penggunaan UPS, tersedia racun

api di beberapa titik, tersedia ginset, memasang anti petir, penggunaa password dan akun tiap-tiap karyawan dan terdapat larangan merokok di seluruh rumah sakit.

2. Berdasarkan hasil penelitian, mitigasi risiko yang harus di lakukan RSIA Eria Bunda adalah dengan melakukan pengadaan komputer khusus server dan pengadaan ruangan khusus server untuk menghindari risiko tertinggi yang teridentifikasi.

Saran

Pada dasarnya TI RSIA Eria Bunda sudah menerapkan manajemen risiko, tetapi tidak secara terstruktur dan terdokumentasi. Maka dari itu di harapkan penelitian ini bisa menjadi modul untuk TI RSIA Eria Bunda melakukan manajemen risiko sistem informasi secara terstruktur dan terdokumentasi. Adapun saran yang di sampaikan oleh peneliti adalah :

1. Sebaiknya ada dana khusus yang di alokasikan RSIA Eria Bunda untuk melakukan manajemen risiko sistem informasi, karna manajemen risiko sistem informasi seharusnya berjalan terus-menerus selama organisasi itu menerapkan teknologi informasi pada proses kerja nya.
2. Yang paling penting adalah manajemen risiko sistem informasi dapat berjalan dengan baik jika di dukung dengan komitmen manajer senior dan di dukung penuh dari seluruh karyawan yang harus mengikuti prosedur dan kontrol yang telah di terapkan.
3. Sebaiknya untuk penyempurnaan penelitian selanjutnya, framework NIST SP 800-30 di sandingkan dengan framework lain karna banyak unsur dari framework lain yang bisa di sandingkan dengan NIST SP 800-30 yang bersifat minor maupun mayor, dengan begitu kekurangan yang ada pada framework ini dapat di isi dengan unsur dari framework lain berdasarkan kebutuhan penelitian.

DAFTAR PUSTAKA

Blokdijk, G, dkk. (2008). IT Risk Management Guide: RiskManagement Implementation Guide, Presentations, Blueprints, Templates. AU: Emereo Pty Limited.

Darmawi, Herman. (2006). Manajemen Risiko. Jakarta: BumiAksara.

Depkes RI, 2009 , <http://depkes.go.id>. Dikutip tanggal 12 juli 2019.

Djohanputro, B. (2008). Manajemen Risiko Korporat. Jakarta: PPM.

Djojosoedarso, Soeisno. (2009). prinsip-prinsip Manajemen Risiko dan Asuransi. Jakarta: Salemba Empat.

Gibson, Danil. (2011). Managing Risk in Information Systems. Sudbury: Jones & Bartlett Learning.

Gondodiyoto, sanyoto. (2007). Audit Sistem Informasi Pendekatan COBIT. Jakarta: Penerbit Mitra Wacana.

Hanafi, Mamduh. (2009). M. Manajemen Risiko.yogyakarta: UUP STIM YKPN.

Hidayat, Resmiadi. (22016). Manajemen Risiko Terhadap Sistem Teknologi Informasi Menggunakan NIST dan COBIT 5.

Hopkin, Paul. 2010. Fundamentals of Risks Management : Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page. London.

Idroes, F. N. (2008). Manajemen Risiko perbankan: Pemahaman Pendektan 3 pilar Kesepakatan Bassel II Terkait Aplikasi Regulasi dan Pelaksanaannya di Indonesii. Jakarta: Rajawali Pers.

Istiningrum. (2011). Implementasi Penilaian Risiko dalam Menunjang Pencapaian Tujuan Instansi Pendidikan. UNY.

Jogiyanto. (2005). Analisis Desain Sistem Informasi. Yogyakarta: Andi.

Joint Task Force Transformation Initiative. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. NIST Special Publication 800-39.

Jordan, E. & Silcock, L. (2005). Beating IT Risks. England: John Wiley and S

Maulana, & Supangkat. (2006). Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. Prosiding Konferensi

- Nasional Teknologi Informasi & Komunikasi untuk Indonesia, 121-126.
- Mauliza, Rizki. (2018). Manajemen Risiko Sistem Informasi Perpustakaan Sekolah Tinggi Ilmu Pertanian Agrobisnis Perkebunan (Studi Kasus BPSDM Jawa Barat). Universitas Sumatera Utara
- Novianti. (2018). Analisis Manajemen Risiko Sistem Informasi KKN Universitas Lampung Menggunakan Metode NIST SP 800-30. Bandar Lampung
- Nugraha, U. (2016). Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-30. Bandung: SELISIK.
- Nurochman, A. (2014). Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus Di Perpustakaan Universitas Gadjah Mada Yogyakarta). Yogyakarta: BIPI.
- Oetomo, Budi Sutedjo Dharma. (2002). Perencanaan dan Pembangunan Sistem Informasi. yogyakarta: Penerbit:Andi. Perwita, Machruniza Anggi.
- Bagaimana Penanganan Inventaris Aset Menurut ISO 27001:2013.*
<https://itgid.org/bagaimana-penanganan-inventaris-aset-menurut-iso-270012013/>.
 Dikutip 12 Juli 2019
- Pinontoan, J. H. (2010). Manajemen Risiko TI Konsep-konsep. Majalah PC Media.
- Sinurya, Kristina (2016, 17 Juli).
- Peran Sistem Informasi Rumah Sakit Dalam Pelayanan Keperawatan.*
<https://www.kompasiana.com/khristinasinuraya/578b4689c3afbfd307b48d00/peran-sistem-informasi-rumah-sakit-sirs-dalam-pelayanan-keperawatan>. Dikutip 12 Juli 2019
- Siregar, C.J.P, 2003. *Farmasi Rumah Sakit Teori & Penerapan*. Jakarta : EGC
- Siswanto, R & Luther, R. 2011. Pengukuran Manajemen Risiko Sistem Informasi Menggunakan Metode OCTAVE-S Studi Kasus Pada PT. XYZ, 3 Februari.
- Solihin. (2019). Manajemen Risiko Sistem Informasi Pelaporan Sortasi Online Pada PT. Perkebunan Nusantara V Menggunakan Metode National Institute of Standart and Technology Special Publication 800-30". Pekanbaru: UMRI.
- Stoneburner G, A. Goguen and A. Feringa. (2002). Risk Management Guide for Information Technologist Systems., Reocommendation of the National Institute of : Standart and Technology Special Publication 800-30.
- Tantra, Rudy. (2012). Manajemen Proyek Sistem Informasi. Yogyakarta: Penerbit: Andi.
- Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit.
- Valena, Danis. (2018). Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode NIST SP 800-30. Bandar Lampung
- Wikipedia. (3 Spetember 2017). "ISO/IEC 27001.
https://id.wikipedia.org/wiki/ISO/IEC_27001. (Dikutip 12 Juli 2019)
- Wolingpirayat, J. (2007). E-payment Strategies of Bank Card Innovation. Journal of Internet Banking And Commerce.
- Yasa, W. W., Dharma, I. G. B. S. & Sudipta, I. G. K. 2013. Manajemen Risiko Operasional Dan Pemeliharaan Tempat Pembuangan Akhir (TPA) Regional Bangli di Kabupaten Bangli, Juli. Volume 1.
- Yustira. Amelia (2017). Sistem Informasi Rumah Sakit Rumah Sakit Umum Daerah Gumawang Dengan Menggunakan Java Server Pages (JSP). Universitas Islam Negeri Raden Fatah Palembang.